

AIR WAR COLLEGE

AIR UNIVERSITY

BUREAUCRACY VS. BIOTERRORISM: COUNTERING A GLOBALIZED THREAT

by

Stephen G. Hoffman, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

16 February 2011

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 16 FEB 2011		2. REPORT TYPE		3. DATES COVERED 00-00-2011 to 00-00-2011	
4. TITLE AND SUBTITLE Bureaucracy vs. Bioterrorism: Countering a Globalized Threat			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air War College,325 Chennault Circle,Maxwell AFB,AL,36112			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 27	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

I. INTRODUCTION	5
II. CONFLUENCE OF TECHNOLOGIES	3
Definitions and Background	3
Advancing Rate of Development	5
Shopping List for a DIY Bioterrorist	8
What Failure Looks Like	10
III. REINFORCING NORMS OF RESPONSIBLE CONDUCT	12
Police within Profession	12
Increase Attribution	14
Mitigate Consequences	15
IV. RECOMMENDED ADDITIONAL AF STUDY	17
How Many Life Science Officers are Enough?	17
How Should Information Cross-Flow Occur?	18
Is Life Science Certification Necessary?	18
V. CONCLUSION – A NETWORK OF COUNTERMEASURES	19
BIBLIOGRAPHY	21

Biography

Lieutenant Colonel Stephen G. Hoffman is a student at the Air War College, Maxwell AFB, Alabama. Colonel Hoffman enlisted in the Air Force in 1984 as a KC-135 aircraft mechanic and was later commissioned a Second Lieutenant in 1989 through the Air Force Reserve Officer Training Corps. He is an Operations Research Analyst who has served in a variety of positions including Enlisted Personnel Analyst, Operational Test Manager, Scientist Assignment Officer and Division Chief, Force Structure Assessments on the Air Staff; he has also completed broadening assignments as a Major Command Financial Analyst and Comptroller Squadron Commander which culminated in his selection by the Assistant Secretary of the Air Force for Financial Management, as the Comptroller of the Year for 2007. He is a graduate of the Air Force Institute of Technology with a Master of Science Degree in Operations Research. Prior to his assignment to the Air War College, Lieutenant Colonel Hoffman was the Acquisition and Space Colonel Assignment Officer, Pentagon.

I. INTRODUCTION

Two things are certain: death and taxes! Or maybe just taxes. Scientists are attempting to cheat death with rapidly progressing technologies capable of constructing and manipulating life synthetically from basic chemical elements. While the advancing rates of capability in computing speed, genomics, synthetic biology and nanotechnology have the potential to improve and lengthen life for all humans, they also enable biological weapons that can destroy wide swaths of humanity or attack specific groups of individuals. This confluence of technology is advancing at exponential rates and seems have the advantage over the limited detection, protection and treatment capabilities offered by a lumbering bureaucracy.

While human nature has not changed, rapidly advancing technology is providing new and novel biothreats to our adversaries. Globalization and the increasing availability of knowledge required to develop biothreats coupled with declining computing costs work together to dramatically increase the likelihood of biological weapon proliferation over the next 25 years. Given a future proliferation of biological weapons to terrorist groups facilitated by globalization and rapidly increasing technological advancements, can a bureaucracy develop an effective network of countermeasures to bioterrorism?

Developing a network of credible countermeasures requires a consistent demonstration of intent to defeat bioterrorists backed by a viable capability. Intent to counter bioterrorism must be communicated to both potential terrorists as well as scientists who may be vulnerable to terrorist propaganda. Scientists considering facilitating terrorists with technical support needed to develop biological weapons may be deterred through professional pressure by their peers in the life science community. The medical profession has long had a concentration of knowledge which, if used wrongly, had the capacity of harming the very patient needing care. Even with

this potentially dangerous information, trained medical personnel have developed a set of standards efficiently applied across their professional community. Perhaps the life sciences professions can increase acceptable behavior through adopting a similar ethic, code of standards and self-policing professional community.

In addition to efforts to deter individuals through professional peer pressure, a credible network of countermeasures will include the ability to detect and attribute unacceptable activity. Scientists secretly working to develop biological weapons for terrorists may be further influenced to return to the mainstream if their work is detected and attributed to them directly. Attribution has the effect of removing anonymity from those bioterrorists who might otherwise believe they are impervious to retribution. With removal of anonymity through increased attribution, rogue scientists may be influenced to stop their unprofessional behavior.

Finally, communicating intent to defeat bioterrorists rings hollow if there is no capability to deny the potential terrorists their desired end state or to coerce them with a believable expectation of punishment. Mitigating consequences of biological weapons is one way to deter would-be terrorists. A demonstrated ability to quickly react and counteract the effects of a biological weapon would remove the reward that a terrorist desires. Establishment of quick reaction teams capable of identifying the threat and developing treatment with use of nanotechnology for mass aerosol inoculation may show how the U.S. is serious about bioterrorism. Furthermore, mitigating consequences can also influence the terrorist on a personal level. That is, effective international law enforcement may increase the risk of incarceration in the same way a quick response team may reduce the reward of mass casualties. Effective development and enforcement of international law is the final aspect of a proposed network of countermeasures to aid bureaucracy in combating a future proliferation of biological weapons.

II. CONFLUENCE OF TECHNOLOGIES

“The convergence of nanotechnology with information technology, biology, and social sciences will reinforce discoveries and innovation ...”¹

--President George W. Bush

Definitions and Background

Three key developing technologies underlying the biothreat environment are genome sequencing, synthetic biology and nanotechnology. The term genome refers to the complete library of information contained on an organism's deoxyribonucleic acid (DNA) or in the case of some viruses, ribonucleic acid (RNA). Both DNA and RNA are constructed with strands (single strand for RNA and usually double strand for DNA) of simple units called nucleotides which in their complete form are referred to as the genomic sequence. The second developing technology, synthetic biology, is “the design and construction of new biological parts, devices and systems [as well as] the re-design of existing, natural biological systems for useful purposes.”² Funded largely through venture capital sources, leading life science experts have already made significant strides toward constructing living organisms synthetically from basic chemical elements. The third developing technology is nanotechnology. “Nanotechnology is a revolutionary technology, growing progressively from rudimentary nanostructures toward molecular nanosystems.”³ Nanotechnology is particularly useful in genomic mapping.

Genomic mapping or sequencing is the first step in identifying sections responsible for disease so that drugs to suppress or counteract that section of the genome can be developed. Simple organisms typically have less complex genomes and higher order organisms have longer genome strands. “In 1990 an international, publicly funded effort, [called] the Human Genome

¹ David M. Burube, *Nano-Hype: The Truth Behind The Nanotechnology Buzz*, Amherst, NY, Prometheus Books, 2006, 130.

² Synthetic Biology. Accessed September 27, 2010. <http://syntheticbiology.org/>.

³ David M. Burube, *Nano-Hype: The Truth Behind The Nanotechnology Buzz*, 17.

Project, was launched to map and sequence human DNA and make the information freely available to the scientific community.”⁴ The project was completed two years ahead of schedule in 2003, and the pace of growth in genome sequencing has continued to increase.

Secondly, synthetic biology has also seen rapid gains in development. “Synthetic [biology] comes in two broad classes. One uses unnatural molecules to reproduce emergent behaviours from natural biology, with the goal of creating artificial life. The other seeks interchangeable parts from natural biology to assemble into systems that function unnaturally.”⁵ In July 2002, beginning only with a genomic sequence of a single strand RNA, researchers created and activated a virus identical in appearance and effect to naturally occurring polio.

The third technology impacting the biothreat environment is nanotechnology, which refers to development of capabilities by scientists to manufacture on a molecular level. A nanometer is one-billionth of a meter which is about five or ten times as long as the width of an atom. “What is interesting about nanotechnology is that it functions as a technological multiplier.”⁶ That is, nanotechnology itself is merely a facilitator of synthetic biology providing tools and processes required to manipulate genomic strands. A U.S. Department of Agriculture report identifies detection of pathogens as one of many potential applications of nanotechnology.⁷ Lawrence Berkeley National Laboratory scientists are capitalizing on the advancing rate of technology by developing “sensor systems that both detect nanoparticles and rely on the formation of nanoparticles that have been developed as sensing species.”⁸ Obviously, a strategy countering bioterrorism is further complicated by continuing advances in these areas.

⁴ John Sulston and Georgina Ferry, *The Common Thread: A Story of Science, Politics, Ethics, and the Human Genome*, Washington D.C., Joseph Henry Press, 2002, viii.

⁵ Steven A. Brenner and A. Michael Sismour, “Synthetic Biology,” *Nature Reviews: Genetics*, Vol. 6, Jul 2005, 533.

⁶ David M. Burube, *Nano-Hype: The Truth Behind The Nanotechnology Buzz*, 22.

⁷ *Ibid.*, 193.

⁸ Sensors Group, Lawrence Berkeley National Laboratory, http://sensors.lbl.gov/sf_nano.html, accessed Dec 2010.

Advancing Rate of Development

The rapid progress in genomics, synthetic biology and nanotechnology has surprised many professionals in the life science fields and the overwhelming consensus is that the pace of advancement is likely to increase. Beneath all three of these technologies is the unmistakable linkage between increasingly powerful computers and advances in genomic sequencing, synthetic biology and nanotechnology. The synergistic effect of technological advancement coupled with increasingly powerful computers offer incredible commercial returns on investment while simultaneously increasing the risk of biothreat proliferation.

Kurzweil showed in *The Singularity is Near*, how microprocessor clock speeds have followed an increasing exponential trend line doubling every three years since 1975, while over the same period microprocessor costs (per transistor cycle) have followed a declining exponential trend line (Figure 1); cutting their costs in half every 1.1 years.⁹ This trend affects

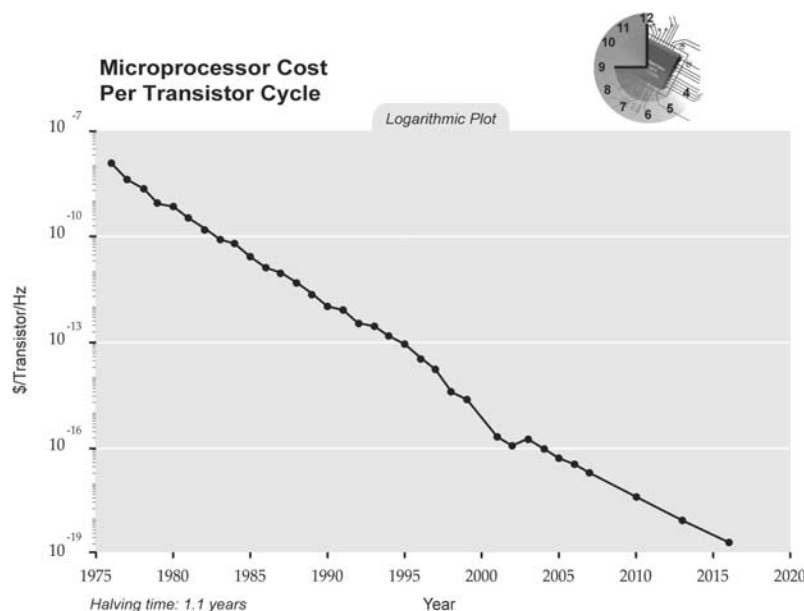


Figure 1. Microprocessor Cost per Transistor Cycle¹⁰

⁹ Ray Kurzweil, *The Singularity is Near: When Humans Transcend Biology*, New York, NY, Viking Penguin Books, 2005, 61-62.

¹⁰ Ibid., 61.

development of genomic and synthetic biology directly as both of these fields are dependent on powerful computers to process the enormous DNA sequencing code, and indirectly as a function of cost. That is, biotech companies are much more likely to receive venture capital where the cost-to-profit ratios are greatest.

Beginning in 1980, with the Human Genome Project, rates of increase in genomic sequencing and synthetic biology (Figure 2) appear to be following similarly explosive growth patterns. The Institute of Medicine and National Research Council states, “[t]he accelerating pace of discovery in the life sciences has fundamentally altered the threat spectrum.”¹¹ The dramatic decrease of sequencing costs per pair of nucleotides, is driven by two factors.

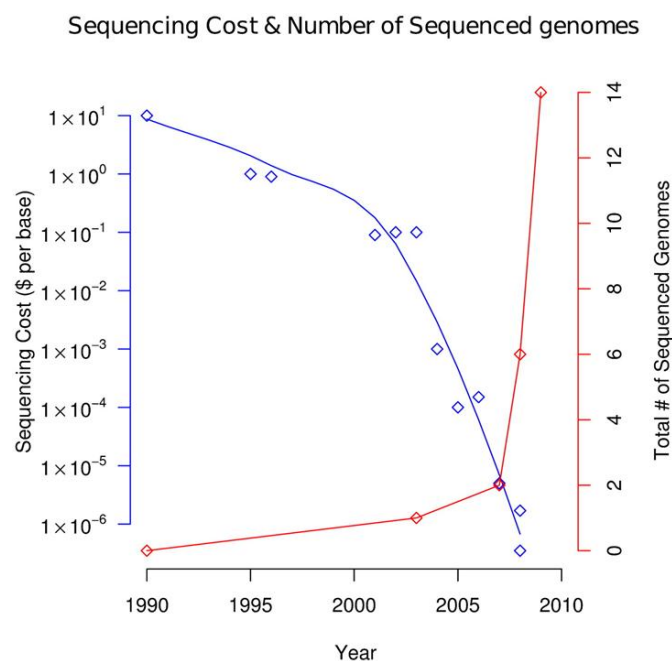


Figure 2. Sequencing Cost and Number of Sequenced Genomes¹²

First, the decreasing cost of computing power is making the hardware aspect of the process less expensive. Second, software or process improvements that come as a result of scientific

¹¹ Institute of Medicine and National Research Council of the National Academies, *Globalization, Biosecurity, and the Future of Life Sciences*, Washington D.C., The National Academies Press, 2006, 5.

¹² Michael Snyder, Jiang Du and Mark Gerstein, “Personal Genome Sequencing: Current Approaches and Challenges,” <http://genesdev.cshlp.org/content/24/5/423.full>, accessed 18 Nov 2010, Figure 1.

discovery raise the baseline across the industry. These two factors are complimentary in that, as computing costs go down more sequencing is being done by more companies; and as the scientists at these companies learn, compete and develop more efficient processes, the overall cost per sequenced genome pair plummet aggressively. Similar reasoning applies for why the total number of sequenced genes has rapidly increased. The economics of computing, genomics and synthetic biology show no sign of slowing.

A price performance curve for nanotechnology cannot be displayed in a manner similar to microprocessor costs, genomic sequencing costs or number of sequenced genomes since nanotechnology refers to the molecular scale rather than a specific technology. Figure 3 does, however, indicate the rapidly increasing pace of U.S. Government funding for nanotechnologies across the first ten years of this century. While the increase in funding has followed a relatively linear incline, the average annual increase over these ten years is 23%. Cumulatively, this results in a 465% increase in federal funding for nanotechnology between 2000 and 2009. Given the

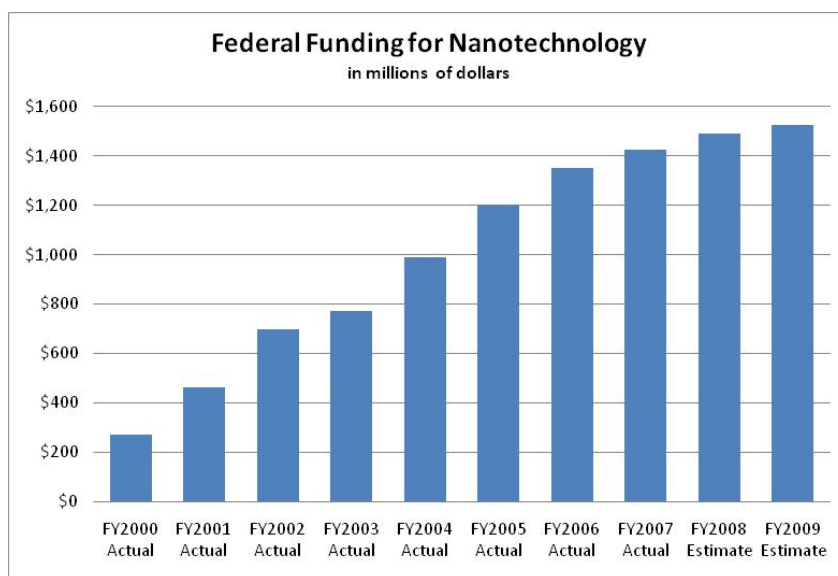


Figure 3. Nanotechnology Funding, by Agency: FY2001-FY2008 & FY2009 Request¹³

¹³ John F. Sargent Jr, "The National Nanotechnology Initiative: Overview, Reauthorization, and Appropriations Issues," *Congressional Research Service*, 7-5700, RL34401, 6 May 2009, 16.

austerity of federal funding over this period, an average annual increase of 23% is quite significant. Of course the federal government is not the only funding source for nanotechnology, but this data does emphasize the point that along with computing cost efficiencies, and genomic and synthetic biology advancements, nanotechnology enables exponentially growing advances in life sciences by facilitating smaller, cheaper and faster computing.

Shopping List for a DIY Bioterrorist

One consequence of increasingly cost efficient computing power coupled with advances in genomics, synthetic biology and nanotechnology is that do-it-yourself (DIY) genetic engineering is entering the realm of the possible. Barry Pallotta and Michael Finnin at the Institute for Defense Analyses detailed how DIY biologists can use everyday items, shown in Figure 4, to attain rudimentary biological engineering capabilities. With very little effort

Professional	Do-It-Yourself
Gel Electrophoresis	Drinking Straws, 9V Batteries, Food Grade Agar
Pipettor	Coffee Stirrer
Electroporator	Ultrasonic Jewelry Cleaner
Centrifuge	Dremel-Fuge, Coffee Grinder
Temperature Bath	Pot of Warm Water
PCR Thermocycler	3 Pots of Warm Water
Autoclave	Pressure Cooker
CO ₂ Cell Incubator	CO ₂ from Vinegar and Baking Soda
Enzymes and Solvents	Household Chemicals
Analytical Balance	Jewelry/ food Scale (mg Precision)

Figure 4. DIY Biologist Laboratory using Household Items¹⁴

searching online auction sites like eBay, the DIY biologists can greatly enhance their basement laboratories with a strikingly small financial investment. This proliferation of inexpensive technological hardware is an unexpected by-product of globalization that offers alternatives to otherwise prohibitively expensive scientific equipment previously available only to universities

¹⁴ Barry S. Pallotta and Michael S. Finnin, "DIY Biology: Capabilities Assessment," *Institute for Defense Analyses Internal Study: CRP-2139*, For Government Use Only, 4 May 2010, slide 9.

and government organizations. Armed with only online access and \$1,000, the DIY biologists can purchase professional equipment like the following recently advertised on eBay:

Temperature bath - \$150, Cell incubator - \$230, PCT Thermocycler - \$200, Centrifuge - \$100.

There are, however, limits to the DIY biologists as their learning and capabilities are only facilitated by the successes of the professional biomedical community. The DIY community has achieved only level three, of the nine levels of technical complexity shown in Figure 5, while PhD level professionals in the biomedical community have achieved level seven. Even though the capabilities of DIY biologists are significantly lower than the professional community, technical advances are making this a viable concern for the future. The potential damage of malicious or accidental biological pathogen release by biologists outside the professional community is becoming more likely with the proliferation of inexpensive technology.

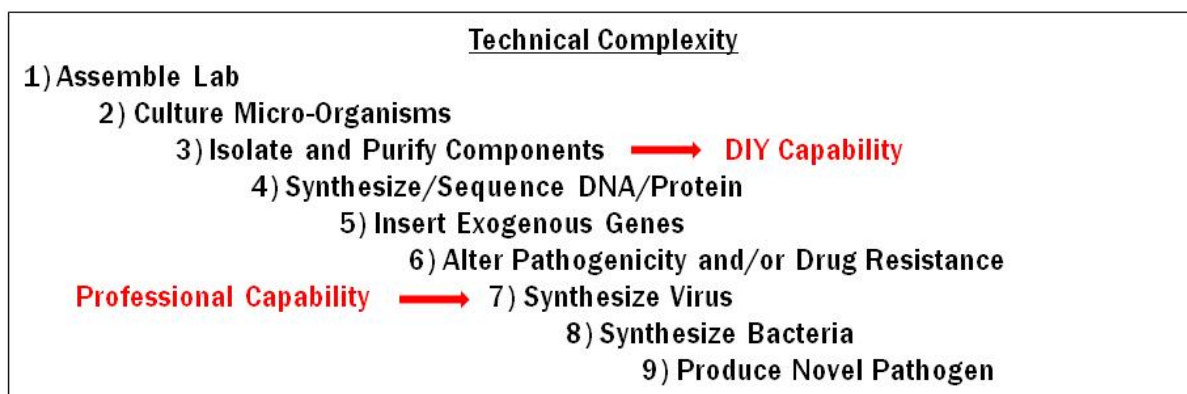


Figure 5. Biocapability Technical Complexity Levels 1-9¹⁵

The DIY community has yet to independently sequence or synthesize DNA similar to results of the (1990-2003) Human Genome Project. Following the successful Human Genome Project, the professional community compiled numerous additional successes for the following eight years (2003-2011), culminating in viral synthesis. While the professional community

¹⁵ Barry S. Pallotta and Michael S. Finnin, "DIY Biology: Capabilities Assessment," slide 17.

required 13 years to sequence DNA and 8 additional years to synthesize a virus, the DIY community benefits from a dispersion of knowledge through published scientific reports. Estimating (very conservatively) a 10-20 year lag behind the professional community, DIY biologists are likely to obtain technical complexity level seven or eight by 2035. Given the advancing pace of development across genomics, synthetic biology and nanotechnology, an estimated technical complexity level nine, for the DIY community, is not at all unreasonable. Failure of bureaucracy to develop a novel network of countermeasures against DIY scientists and would-be bioterrorists, who can wage warfare from Walmart, is foolhardy.

What Failure Looks Like

Globalization and the Internet have enabled widespread distribution of technical knowledge and hardware, and there is no way to put the genie back in the bottle. Relying solely on traditional deterrent policies against a globally proliferated biothreat will not suffice when attempting to counter a technology-empowered bioterrorist. If the bureaucracy can ever hope to develop an effective network of countermeasures to bioterrorism, then certainly the first step in that development is an accurate assessment of the consequences of what failing to do so would have on the United States. Andrew Krepinevich, in the “Pandemic” chapter of his 2009 book, 7 *Deadly Scenarios*, provides a glimpse of how that failure might look.

“Meanwhile, as the United States increasingly resembles a vast collection of semi-ghost towns, to the south literally millions of peoples are on the move. ... This mass of Mexicans, now estimated at nearly eight million, has no organizing force directing it, yet all its participants are unified toward one goal: crossing the border into the United States, in hope of gaining access to this country’s medical system – which ironically in many ways has simply ceased functioning in any meaningful way. This mass migration is ... driving Mexico’s population north – a human tidal wave about to crash across America’s borders.”¹⁶

¹⁶ Andrew F. Krepinevich, *Seven Deadly Scenarios: A Military Futurist Explores War in the 21st Century*, New York, NY, Bantam Dell, 2009, 92.

A bioterrorist attack on the U.S. could take the form of an introduction of a mutated Avian Flu virus, capable of being passed human-to-human, into unsanitary villages in Mexico. Poor surveillance by the World Health Organization, coupled with typical American disbelief of vulnerability to a pandemic, would likely permit early reports of 10, 20 or 50 deaths scattered across Mexican villages to go largely unnoticed in the United States. One characteristic of viral growth is its exponential increase, so these seemingly small and scattered deaths could, within weeks, ramp into millions of cases of Avian Flu. Even though the Spanish Influenza of 1918 killed 675,000 Americans and estimates of an Avian Flu pandemic are that 2,000,000 could die, the Center for Disease Control (CDC) has failed to develop sufficient antiviral stockpiles.

“The combination of the pandemic, the lack of government preparedness, and sensationalist media [would diminish American’s] confidence and trust in their government.”¹⁷ Furthermore, the second and third order effects of a pandemic, coupled with global mobility, may be increased gang activity, looting and violent crime worldwide such that implementation of martial law may be required. Overwhelmed governments may attempt to clamp down on individual rights to free speech and assembly if mob violence were to spontaneously erupt anywhere social networks indicated medical supplies existed. In the U.S., the President would likely nationalize all antiviral treatments under the direction of the CDC, Federal Emergency Management Agency and the Department of Defense. Since “95 percent of the world’s vaccine is produced by countries comprising only about 10 percent of the world’s population,”¹⁸ minority groups may characterize the President’s nationalization of medical supplies as nothing more than opportunistic ethnic cleansing. In light of these global implications to bioterrorism it is imperative that the U.S. show leadership in propagating ethical norms of responsible conduct.

¹⁷ Andrew F. Krepinevich, *Seven Deadly Scenarios: A Military Futurist Explores War in the 21st Century*, 99.

¹⁸ *Ibid.*, 113.

III. REINFORCING NORMS OF RESPONSIBLE CONDUCT

“We will work with domestic and international partners to protect against biological threats by promoting global health security and reinforcing norms of safe and responsible conduct;...expanding our capability to prevent, attribute, and apprehend those who carry out [bio]attacks.”¹⁹

--President Barack Obama

Police within Profession

The education, training and skills of scientists in biology, chemistry and genetics empower life science professionals with capabilities that must be used according ethical standards of professional peer organizations. Pledging an oath to publically state one's agreement and voluntary self-censorship according to the guidelines of the group's ethical standards is an effective way of bonding a member to his or her profession. The very word “profession” in its Latin origin means ‘bound by an oath’.²⁰

“Nearly all medical schools incorporate some form of professional medical oath into their graduation ceremonies. The oldest and most popular of these oaths is the Hippocratic Oath, composed more than 2,400 years ago.”²¹ In addition to medical doctors, oaths have been adopted in many other professions to build a commitment to the group which encourages and polices ethical actions. When these oaths are additionally printed and signed there is an even greater level of buy-in on the part of the member. Individuals who profess such an oath are motivated primarily by altruistic desires, but negative reinforcement from peer reproach also encourages proper behavior.

¹⁹ Barack H. Obama, *National Security Strategy*, Washington D.C., Government Printing Office, May 2010, 24.

²⁰ Daniel Fu-Chang Tsai, and Ding-Shinn Chen, “An Oath for Bioscientists,” <http://www.ncbi.nlm.nih.gov/pubmed/14576458>, accessed 18 Nov 2010, 571.

²¹ Raphael Hulkower, “The History of the Hippocratic Oath: Outdated, Inauthentic, and Yet Still Relevant,” *The Einstein Journal of Biology and Medicine*, Albert Einstein College of Medicine, Bronx, NY, 41.

Additionally, the professional communities to which members pledge an oath provide tangible value to those members in the form of certification and peer recognition. The very nature of professions with unique education and training necessitates a very precise vernacular not often understood by the layman. When a member demonstrates proficiency through testing or peer review, a certification may be granted, externally validating this member. While outsiders may not understand the particular language or nuances of the profession, certification is often sufficient for promotion or advancement. It follows then; potential loss of a professional certification may also act as a deterrent to unapproved activity.

Due to the danger of globalized technological advancements in the life sciences arena even peer review maybe insufficient to safeguard against biothreats. “Sir Joseph Rotblat, the 1995 Nobel Peace Prize laureate, urged in his acceptance speech that ‘the time has come to formulate guidelines for the ethical conduct of scientists, perhaps in the form of a voluntary Hippocratic Oath’.”²² Developing and implementing guidelines in the form of an oath would help fulfill President Obama’s mandate of protecting against biothreats while “reinforcing norms of safe and responsible conduct.”²³

There are limitations, however, to the effectiveness of professional policing. Western professionals are motivated to ethical activity through a compelling system of reward and punishment from a linear-active society that places great value on both words and deeds. Societies valuing tribal, ethnic or religious relationships more highly than ethical codes will not provide the ethical underpinning necessary for professional policing. Therefore a second capability must be added to the proposed bureaucratic network against bioterrorism; increased attribution to find and expose those who do not follow the professional code.

²² Daniel Fu-Chang Tsai, and Ding-Shinn Chen, “An Oath for Bioscientists,” 569.

²³ Barack H. Obama, *National Security Strategy*, 24.

Increase Attribution

Detection of bioterrorism is a collective activity heavily dependent on physical evidence acquired through material sensors, whereas attribution demands a higher level of effort as both capacity and intent must be shown. Detection is the tool for validating enemy capacity toward biothreat development, testing or use. Attribution demands evidence that not only is there an adversary involved in some stage of biothreat activity, but that that adversary also intends to use that biothreat as a weapon. Researchers at University of Florida are developing a nanotechnology that may aid with both detection and attribution and provide at least one avenue towards removing anonymity. These researchers are developing a ‘smart dust’ that changes color when exposed to precursor elements of biological weapons.²⁴

Attribution can continue to be an effective aspect of the national security strategy even for individual bioterrorists if the strategy is applied with understanding from the perspective of the adversary. Deterrence through attribution requires the capability to detect and attribute bioterrorist activity coupled with credibility to deny or punish adversaries’ efforts. Attribution has the effect of removing anonymity from bioterrorists who might otherwise believe they are impervious to retribution. An experiment validating this conclusion by psychologists Zhong, Bohns, and Grino showed how volunteers in a dimly lit room were decidedly more likely to lie, cheat and steal than volunteers in a brightly lit room. In this experiment, darkness provided the anonymity which facilitated criminal activity.²⁵

²⁴ Lynn E. Foster, *Nanotechnology: Science, Innovation, and Opportunity*, Upper Saddle River, NJ, Prentice Hall, 2006, 218.

²⁵ Chen-Bo Zhong and Vanessa K. Bohns and Francesca Gino. “Good Lamps Are the Best Police: Darkness Increases Dishonesty and Self-Interested Behavior.” *Psychological Science*. First published online 29 January 2010, DOI: 10.1177/0956797609360754, <http://pss.sagepub.com/content/early/2010/01/28/0956797609360754.abstract>, accessed 18 Nov 2010.

Use of smart dust as a nanotaggant may, as an example, serve as a means of removing anonymity of those working with precursor elements of biological weapons. That is, a rogue scientist experimenting with the building blocks of biological weapons may be deterred from further effort if his tools, workplace, hands and clothing all fluoresce; letting him know that he is not as anonymous as he may have thought. Should the color-changing smart dust not deter the wayward scientist, then policing from his professional community may discourage continued development of biological weapons.

A broad array of collection tools and techniques add flexibility to detection capabilities which in turn enhances the ability to attribute developing threats from would-be bioterrorists. In cases where both loss of anonymity and professional policing fail to dissuade rogue scientists then use of nanoparticles may mitigate the consequences as tagging identifiers for criminal apprehension and prosecution. Mitigation of consequences is the third capability necessary for the proposed bureaucratic network against bioterrorism. This capability is comprised of a two-prong effort to counter bioterror activity; effective counteraction of biothreats and technology enhanced enforcement of international law.

Mitigate Consequences

Aggressively working to mitigate the consequences of a bioterrorist act may deter the act in the first place. One method of mitigating consequences is to develop quick response teams with the proper training and expertise to rapidly counter the effects of a biological weapon. Three essential capabilities of such a quick response team are the ability to: 1) rapidly identify a pathogen used in a bioattack, 2) develop an effective treatment, and 3) administer both treatment and inoculation to the appropriate populations. Quick response teams would mitigate the terrorist's desired reward of causing mass American casualties. Additional mitigation may result

through achieving increased likelihood of capture and punishment to the potential bioterrorist through improved international law and treaties pertaining to life sciences.

Key technologies essential to a quick response team are nanovector therapy and nanosurface technology. In nanovector therapy, an ideal dosage of drug is delivered at full concentration to the intended tissue only. This optimal method of delivery reduces the amount of drug required for treatment while diminishing undesired side effects in tissue or organs where the drug is unnecessary, but might have otherwise been absorbed. Another benefit to the efficacy of this style of drug delivery is that the body's natural defenses can be purposefully bypassed, further reducing collateral damage.²⁶ This technique is partially made possible by nanosurface technologies where drug treatments are covered by protective nanocoatings. The nanosurface technology enables application of coatings that are programmable to dissolve when and where desired. This technique is an adaptation of a naturally occurring coating where pathogens or germs are either repelled or attracted based on the host-organisms requirement.

While these nanotechnologies are still in development, their utility to quick response teams would be invaluable in identifying, treating and inoculating against a biothreat. Using nanotechnology is a necessary technique if any bureaucracy hopes to keep pace with rapidly advancing technologies. Linear thinking about delivery of medical treatment will not suffice when adversaries demonstrate a willingness to use every non-linear attack technique at their disposal. That is, preparations must be made to dispense care using nanotechnologies in a very short period of time with mass aerosol delivery of nanosurface encapsulated antibiotics or inoculation to effectively mitigate a terrorist's desired outcome. Nanotechnologies may even aid in improved international law application through single molecule detecting sensors. If smart

²⁶ M. Farrari, "Nanovector Therapeutics," *Journal Article Research Support*, U.S. Government, PHS Review, 2005, <http://www.ncbi.nlm.nih.gov/pubmed/15967706>, accessed 18 Nov 2010.

dust nanosensors were made available in the hunt for forensic evidence of a bioterrorist act, this smart dust may actually deter terrorism through increased risk of capture and punishment.

IV. RECOMMENDED ADDITIONAL AF STUDY

The AF can contribute to President Obama's biothreat strategy through increased emphasis on attribution and detection. Therefore, technological developments in genomics, synthetic biology and nanotechnology will be important as the AF strives to fully understand the capability and intent of U.S. adversaries; and when punitive actions are necessary, use of nanotaggant identifiers for targeting of kinetic weapons. There are, however, a few unanswered questions with respect to pragmatic implementation of a bureaucratic network of biothreat countermeasures.

How Many Life Science Officers are Enough?

As of Jan 2010, the total number of active duty officers in the Air Force was 65,515 with only 108 (or 0.17%) identified as biologists or chemists. These scientists were assigned primarily to acquisition organizations supporting programs instrumental to development of biological weapon analysis or detection tools. Near-term increases in life sciences personnel resources may contribute significantly toward leading-edge detection capabilities facilitated by the same technology that is increasing biothreat likelihood. While only 0.17% of all active duty officers trained and employed as life scientists seems paltry, the correct number of truly necessary life science officers is currently unknown. A full investigation of the life sciences personnel requirement is recommended to determine the appropriate number of chemists and biologists required in the scientist officer core.

How Should Information Cross-Flow Occur?

Acquisition and intelligence units currently have no mandated flow of information ensuring the scientific efforts to improve bio-collection are broadly included into future acquisition programs. Likewise, there is no institutionalized flow of information from medical officers to the intelligence and acquisition communities to capitalize on their knowledge of medically related advances in synthetic biology. Developing a mechanism for cross-functional communication between the intelligence, medical, scientific and acquisition communities may increase the likelihood that the latest developments in life science fields are relayed back to acquisition program offices. Institutionalizing this feedback may also formalize the communication with the goal of ensuring the most relevant detection techniques are considered for incorporation into developing programs. It is recommended that the intelligence, acquisition, medical and scientific career fields' functional communities investigate an institutionalized cross-flow mechanism for efficient distribution of the most current life science information.

Is Life Science Certification Necessary?

All three aspects of the proposed network of countermeasures, professional policing, increasing attribution and consequence mitigation, may be facilitated by a well-documented professional life science community. In some instances scientists may self-police if they believe a sanctioning body might remove a professional license should they be caught breaking an ethical code or professional oath. An increased awareness of scientists' professional activity, resulting from a certification process, may very likely increase attribution capabilities. Additionally, international life science laws and treaties may be more effectively enforced by a cadre of externally certified life science professionals. It is therefore recommended that an industry-accepted certification plan for life sciences officers be developed and implemented.

V. CONCLUSION – A NETWORK OF COUNTERMEASURES

Genetics, synthetic biology and nanotechnology are established technologies that have shown incredible rates of advancement. These rates of advancement in the life sciences are anticipated to accelerate even faster, facilitating further developments which make proliferation of biological threats by 2035 almost certain. However, even in a future where biological weapons are proliferated to terrorists through globalization and technological advancements, a bureaucracy can indeed develop an effective network of countermeasures to bioterrorism.

The first aspect of this network is professional policing among life science professionals through development of an oath of ethical actions. A life science oath would “reinforce norms of safe and responsible conduct”²⁷ while also creating ethical standards within the profession. The second aspect in this network is a nanotechnology detection capability to permit unambiguous attribution of bioterrorist activity. This attribution capability may strip anonymity from bioterrorists and coerce them toward civil behavior through the use, as an example, of fluorescing nanotaggants. Knowledge of terrorist actions, once communicated in the light of day, will increase American credibility and deterrent effectiveness through either denial or punishment. The third aspect of this network is mitigation of the consequences of terrorists’ desires though development of quick response teams capable of rapidly identifying pathogens, treating the infected and inoculating the masses through nanovector delivery techniques. Through the use of nanotechnology and improved implementation of international life science laws and treaties, an increased likelihood of punishment to bioterrorists may be realized. Neither the reduction of reward nor increase of risk must be perfect; merely dis-incentivizing the economics of biological weapon use may discourage would-be terrorists from investing effort in this area.

²⁷ Barack H. Obama, *National Security Strategy*, 24.

Developing this network of countermeasures will allow the U.S. bureaucracy to combat bioterrorism by transforming some scientific competitors into collaborators through professional policing. Those who cannot be co-opted by peer pressure may be deterred through a removal of anonymity brought about with technologically enhanced detection and attribution. Finally, bioterrorists undeterred by the loss of anonymity may be compelled to halt their behavior through a two-pronged effort to mitigate biothreat consequences. This consequence mitigation effort would: first decrease a terrorist's motivation by developing quick response teams capable of preventing mass American casualties with nanovector treatment and inoculation, and second by increasing the terrorist's personal jeopardy through nanotechnology-enhanced international law enforcement.

Effective AF participation in this proposed bureaucratic network of countermeasures requires a few foundational questions be answered. To reduce risks of a 2035 biothreat and better support the 2010 National Security Strategy, the AF must: first determine the proper level of scientific personnel required, second institutionalize cross-functional communication across the intelligence, scientific, acquisition and medical functional communities, and third develop an industry-accepted certification program for life science officers. Amid a rapidly changing technological environment, accomplishing these actions now will decrease future risk in the President's overall biothreat strategy by systematically increasing American credibility, capability and communication.

BIBLIOGRAPHY

Brenner, Steven A. and A. Michael Sismour, “Synthetic Biology,” *Nature Reviews: Genetics*, Vol. 6, Jul 2005.

Burube, David M. *Nano-Hype: The Truth Behind The Nanotechnology Buzz*, Amherst, NY, Prometheus Books, 2006.

Farrari, M. “Nanovector Therapeutics,” *Journal Article Research Support*, U.S. Government, PHS Review, 2005, <http://www.ncbi.nlm.nih.gov/pubmed/15967706>, accessed 18 Nov 2010.

Foster, Lynn E. *Nanotechnology: Science, Innovation, and Opportunity*, Upper Saddle River, NJ, Prentice Hall, 2006.

Hulkower, Raphael “The History of the Hippocratic Oath: Outdated, Inauthentic, and Yet Still Relevant,” *The Einstein Journal of Biology and Medicine*, Albert Einstein College of Medicine, Bronx, NY.

Institute of Medicine and National Research Council of the National Academies, *Globalization, Biosecurity, and the Future of Life Sciences*, Washington D.C., The National Academies Press, 2006.

Krepinevich, Andrew F. *Seven Deadly Scenarios: A Military Futurist Explores War in the 21st Century*, New York, NY, Bantam Dell, 2009.

Kurzweil, Ray *The Singularity is Near: When Humans Transcend Biology*, New York, NY, Viking Penguin Books, 2005.

Obama, Barack H. *National Security Strategy*, Washington D.C., Government Printing Office, May 2010.

Pallotta, Barry S. and Michael S. Finnin, “DIY Biology: Capabilities Assessment,” *Institute for Defense Analyses Internal Study: CRP-2139*, For Government Use Only, 4 May 2010.

Sargent, John F. Jr, “The National Nanotechnology Initiative: Overview, Reauthorization, and Appropriations Issues,” *Congressional Research Service*, 7-5700, RL34401, 6 May 2009.

Sensors Group, Lawrence Berkeley National Laboratory, http://sensors.lbl.gov/sf_nano.html, accessed Dec 2010.

Snyder, Michael, Jiang Du and Mark Gerstein, “Personal Genome Sequencing: Current Approaches and Challenges,” <http://genesdev.cshlp.org/content/24/5/423.full>, accessed 18 Nov 2010.

Sulston, John, and Georgina Ferry, *The Common Thread: A Story of Science, Politics, Ethics, and the Human Genome*, Washington D.C., Joseph Henry Press, 2002.

Synthetic Biology. Accessed September 27, 2010. <http://syntheticbiology.org/>.

Tsai, Daniel Fu-Chang and Ding-Shinn Chen, “An Oath for Bioscientists,” <http://www.ncbi.nlm.nih.gov/pubmed/14576458>, accessed 18 Nov 2010.

Zhong, Chen-Bo and Vanessa K. Bohns and Francesca Gino. “Good Lamps Are the Best Police: Darkness Increases Dishonesty and Self-Interested Behavior.” *Psychological Science*. First published online 29 January 2010, DOI: 10.1177/0956797609360754, [http://pss.sagepub.com/content/early/2010/01/28/0956797609360754, abstract](http://pss.sagepub.com/content/early/2010/01/28/0956797609360754.abstract), accessed 18 Nov 2010.